Lecture Notes in Computer Science 10348

More information about this series at http://www.springer.com/series/7410

Sylvain Guilley (Ed.)

Constructive Side-Channel Analysis and Secure Design

8th International Workshop, COSADE 2017
Paris, France, April 13–14, 2017
Revised Selected Papers

Springer

Editor
Sylvain Guilley
Secure-IC S.A.S. and TELECOM-ParisTech
Paris
France

ISSN 0302-9743 ISSN 1611-3349 (electronic)
Lecture Notes in Computer Science
ISBN 978-3-319-64646-6 ISBN 978-3-319-64647-3 (eBook)
DOI 10.1007/978-3-319-64647-3

Library of Congress Control Number: 2017947503

LNCS Sublibrary: SL4 – Security and Cryptology

Printed on acid-free paper

This Springer imprint is published by Springer Nature
The registered company is Springer International Publishing AG
The registered company address is: Gewerbestrasse 11, 6330 Cham, Switzerland

Preface

The 8th International Workshop on Constructive Side-Channel Analysis and Secure Design (COSADE 2017) was organized by and held at Télécom ParisTech, Paris, France, during April 13–14, 2017. The host was the Paris 13th district site of Télécom ParisTech, which is also known as the LTCI (*Laboratoire Traitement et Communication de l'Information*) of Université Paris-Saclay. The workshop was financially sponsored by five golden sponsors, namely, AlphaNov, ANSSI, NewAE Technology, Riscure, and Secure-IC S.A.S. The company INVIA was a silver sponsor of the event.

The excellent arrangements were led by the COSADE 2017 general chair, Prof. Jean-Luc Danger, and organizing chair, Prof. Guillaume Duc. They were helped by a highly motivated team of PhD students from our SEN (*Systèmes Électronique Numérique*) research group, namely, Nicolas Bruneau, Sébastien Carré, Éloi de Chérisey, Margaux Dugardin, Khaled Karray, Damien Marion, Martin Moreau, Alexander Schaub, and Michaël Timbert. This year COSADE provided an open forum for exchanging and sharing of ongoing hot issues and results of research, development, and applications in the analysis of attacks and design of protection against attacks on embedded devices.

The Program Committee prepared for an interesting program, including two invited talks, namely, from Dr. Victor Lomné (ANSSI), talking on "Overview of Fault-based Cryptanalysis on Block Ciphers," and Prof. Philippe Maurine (LIRMM), about the question "Impacts of Technology Trends on Physical Attacks?". The technical program also included an industrial exhibition show, which allowed for fruitful discussions about applications of basic research for transfer to industry.

The workshop had seven sessions built from the contributed papers: on Thursday, "Side-Channel Attacks and Technological Effects," "Side-Channel Countermeasures," "Algorithmic Aspects in Side-Channel Attacks," and on Friday, "Side-Channel Attacks," "Fault Attacks," "Embedded Security," and "Side-Channel Tools."

We would like to thank all authors who submitted papers. Each paper was reviewed by at least three reviewers. The 25 external reviewers as well as the 26 Program Committee members contributed to the reviewing process from their particular areas of expertise. The reviewing and active discussions were facilitated by the EasyChair Web-based system. Through the system, we could check the amount of similarity between the submitted papers and previously published papers to prevent plagiarism and self-plagiarism. Following the strict reviewing processes, 16 outstanding papers from eight countries (Austria, Belgium, France, Germany, Japan, Korea, The Netherlands, and Switzerland) were accepted for publication in this volume of *Lectures Notes in Computer Science* by Springer (LNCS Vol. 10348). I would also like to thank the session chairs (Naofumi Homma, François-Xavier Standaert, Jens-Peter Kaps, Benoît Feix, Benoît Gérard, Yannick Téglia, Pierre-Yvan Liardet, Jean-Luc Danger, and Guillaume Barbu) for their commitment to COSADE.

The workshop featured a welcome reception on the evening of Wednesday April 12, and a social event on board the *Bateaux Mouches* (cruising dinner on the Seine) on Thursday, April 13. During this enjoyable event, François-Xavier Standaert was awarded for the nearest distance with respect to COSADE, and Werner Schindler received the random lottery special prize.

Many people contributed to the success of COSADE 2017. We would like to express our deepest appreciation to each of the COSADE Organizing and Program Committee members as well as the paper contributors. Without their endless support and sincere dedication and professionalism, COSADE 2017 would have been impossible.

May 2017 Sylvain Guilley

Organization

Program Committee

Shivam Bhasin	Temasek Labs@NTU, Singapore
Christophe Clavier	Université de Limoges, France
Hermann Drexler	Giesecke & Devrient, Germany
Cécile Dumas	CEA, France
Thomas Eisenbarth	WPI, USA
Wieland Fischer	Infineon, Germany
Christophe Giraud	Oberthur Technologies, France
Johann Groszschaedl	University of Luxembourg, Luxembourg
Sylvain Guilley	GET/ENST, CNRS/LTCI, France
Benoît Gérard	DGA-MI, France
Tim Güneysu	University of Bremen and DFKI, Germany
Johann Heyszl	Fraunhofer AISEC, Germany
Naofumi Homma	Tohoku University, Japan
Michael Hutter	Cryptography Research, USA
Thanh Ha Le	SAFRAN, France
Kerstin Lemke-Rust	Bonn-Rhein-Sieg University of Applied Sciences, Germany
Houssem Maghrebi	SAFRAN Idendity and Security, France
Marcel Medwed	NXP Semiconductors, Austria
Amir Moradi	Ruhr University Bochum, Germany
Debdeep Mukhopadhyay	IIT Kharagpur, India
Stjepan Picek	KU Leuven, Belgium
Francesco Regazzoni	ALaRI – USI, Switzerland
Matthieu Rivain	CryptoExperts, France
Kazuo Sakiyama	The University of Electro-Communications, Tokyo, Japan
Ruggero Susella	STMicroelectronics, Italy
Carolyn Whitnall	University of Bristol, UK

Additional Reviewers

Alessio, Davide
Bauer, Sven
Bhasin, Shivam
Bocktaels, Yves
Breier, Jakub
Burri, Samuel
Cagli, Eleonora
Chabrier, Thomas
Chattopadhyay, Anupam
Chen, Cong
Dabosville, Guillaume
De Mulder, Elke
Debande, Nicolas
Dinu, Daniel

Grosso, Vincent
Hoffmann, Lars
Jungk, Bernhard
Kavun, Elif Bilge
Le Corre, Yann
Murray, Bruce
Nikov, Ventzi
Patranabis, Sikhar
Pilato, Christian
Prouff, Emmanuel
Reynaud, Léo
Richter, Bastian
Rondepierre, Franck
Saha, Sayandeep
Schneider, Tobias
Seker, Okan
Stöttinger, Marc
Szerwinski, Robert
Tunstall, Michael
Ueno, Rei
Vadnala, Praveen Kumar
Valencia, Felipe
Wenger, Erich
Yamamoto, Dai
Yli-Mäyry, Ville

Contents